REMARKS

A. Introduction

Claims 1-7 and 9-12 were pending and under consideration in the application. Claim 8 was previously cancelled.

In the Office Action mailed January 31, 2011, claims 1-7 and 9-12 were rejected.

With this amendment, no claims are amended.

B. Rejections under 35 U.S.C. §103(a)

Claims 1-2, 4-6 and 9-10 were rejected under 35 U.S.C. §103(a) as being unpatentable over Yap et al., U.S. 6,111,506 (hereinafter "*Yap*"), in view of Kono et al., U.S. 6,813,010 B2, (hereinafter "*Kono*") and in further view of Bridgelall (U.S. Pat. No. 6,672,512) (hereinafter "*Bridgelall*").

Claim 3 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Yap* in view of *Kono*, *Bridgelall* and further in view of Benhammou et al., U.S. 2004/0059925 A1, (hereinafter "*Benhammou*").

Claim 7 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Yap* in view of *Kono*, *Bridgelall* and further in view of Endoh et al., U.S. 2004/0022421 A1, (hereinafter "*Endoh*") and Nick Bromer, U.S. 6,476,715 B1 (hereinafter "*Bromer*").

Claim 11 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Yap* in view of *Kono*, and further in view of *Endoh* and Jerome H. Lemelson, U.S. 4,189,712 (hereinafter "*Lemelson*").

Claim 12 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Yap* in view of *Kono*, and further in view of *Bromer*.

Applicant respectfully traverses all of these rejections.

In relevant part, independent claims 1, 2 and 9 recite an authentication device that mutually authenticates a device storing biological information via a device in communication with the device storing biological information and a management server where the device storing biological data and a device that performs biological authentication exchange encryption data if the mutual authentication is successful.

This is clearly unlike *Yap* and *Bridgelall* which fail to disclose or even fairly suggest this feature. Instead, *Yap* discloses a computer which reads information from a document 10 via an interface unit 64. See, U.S. Pat. No. 6,111,506, Col. 15, l. 20-37. *Bridgeall* discloses central processing system which receives a bar code and an RFID signal from an external device. See, U.S. Pat. No. 6,672,512, Col. 5, . l. 55-Col. 6, l. 12. These references cannot be fairly viewed as disclosing an authentication device which authenticates a device storing biological data via a device in communication with the device storing biological data and the authentication device because the references authenticating data sent from a device without disclosing authentication of a device storing biological information before encryption information is exchanged between two devices.

Kono fails to cure this deficiency. Instead, *Kono* discloses authenticating an image gathered by a hand scanner by matching an image of the user's hand generated by the hand scanner with images stored in a database. See, U.S. Pat. No. 6,813,010, Col. 5, l. 11-27. This cannot be fairly viewed an authentication device that mutually authenticates a device storing biological information and a management server where the device storing biological data and a device that performs biological authentication exchange encryption data if the mutual authentication is successful because *Kono* merely discloses authenticating an image and not a device. As one having ordinary skill in the art would recognize, authenticating an image is not synonymous with mutual authentication of two devices.

Benhammou and *You* also fails to cure this deficiency. Instead, *Benhammou* discloses a card reader and a smart card where the smart card and card reader authenticate each other before performing a read/write operation See, U.S. Pat. Pub. No. 2004/0059925, para. [0008]. You discloses two devices which perform mutual authentication. See, U.S. Pat. Pub. No.

2005/0010769, Para. [0023]. These references cannot be fairly viewed as disclosing an authentication device that mutually authenticates a device storing biological information via a device in communication with the device storing biological information and a management server where the device storing biological data and a device that performs biological authentication exchange encryption data if the mutual authentication is successful because *Benhammou* and *You* merely perform mutual authentication between two devices without disclosing any authentication device, device in communication with the smart card or management server.

The combination of *Kono, Benhammou* and *You* would not produce an authentication device that mutually authenticates a device storing biological information via a device in communication with the device storing biological information and a management server where the device storing biological data and a device that performs biological authentication exchange encryption data if the mutual authentication is successful. As previously discussed, *Kono* is directed at authenticating an image sent, not a device, from a hand scanner where a scanner communicates directly with a database without authentication, *Benhammou* discloses a card reader and smart card performing local authentication without any authentication from a management server and *Yap*, similar to *Benhammou*, discloses two devices performing mutual authentication without any authentication from a management server. Further, none of the references disclose an authentication device.

As the Applicant's specification discloses, by providing an authentication device that mutually authenticates a device storing biological information via a device in communication with the device storing biological information and a management server where the device storing biological data and a device that performs biological authentication exchange encryption data if the mutual authentication is successful, the use of a fraudulent device storing authenticated biological information is prevented. See, U.S. Pat. Pub. No. 2008/0191839, Para. [105]. Accordingly, since the references do not disclose an authenticating unit authenticating the device storing biological data, the references are not capable of a fraudulent device storing authenticated information from being used improperly.

Endoh, Bromer, Lemelson fail to disclose anything pertaining to an authentication device or performing mutual authentication between devices over a network.

Therefore, because *Yep, Kono, Benhammou, Endoh, Bromer, Lemelson* and any possible combination of them fail to disclose or even fairly suggest every limitation of claims 1, 2 and 9, the rejection of claims 1, 2 and 9 cannot stand. Because claims 3-7 and 10-12 depend, either directly or indirectly, from claims 1, 2 and 9, they are allowable for at least the same reasons.

C. Conclusion

In view of the foregoing, it is submitted that claims 1-7 and 9-12 are allowable and early notice to that effect is respectfully requested.

If the Examiner believes that, for any reason, direct contact with Applicants' attorney would help advance the prosecution of this case to finality, the Examiner is invited to telephone the undersigned at the number given below, for purposes of arranging for a telephonic interview. Any communication initiated by this paragraph should be deemed an Applicant-Initiated Interview.

If any further fees are required in connection with the filing of this amendment, please charge the same to out Deposit Account No. 19-3140.

Respectfully submitted,

SNR DENTON US LLP

By: /David R. Metzger/

David R Metzger, Reg, No. 32,919
P.O. Box 061080
Wacker Drive Station, Willis Tower
Chicago, IL 60606-1080
312-876-8000 (telephone)
312-876-7934 (fax)
ATTORNEYS FOR APPLICANT